WE CLAIM:

1. A method of conveying access control information from one network device to another network device on a different domain through an end user device comprising:

the one network device in response to a first message received from the end user device containing access control information, sending a response message to the end user device containing the access control information, the response message being adapted to cause the end user device to send a second message to the another network device containing at least part of the access control information;

wherein at least part of the access control information is used to control access to a protected resource on at least one of the first and second network devices.

2. A method according to claim 1 wherein:

the response message has a header portion and a content portion and the response message contains the access control information and a network device identifier for the another network device embedded within its content portion;

the second message has a header portion and a content portion and the second message contains the at least part of the access control information embedded within its content portion.

3. A method according to claim 1 wherein:

the first message has a header portion and a content portion, and the access control information is contained in the header portion, the method further comprising extracting the access control information from the header portion for use in the response message.

4. A method according to claim 1 wherein:

the first message has a header portion and a content portion, and the access control information is contained in the content portion, the method further comprising extracting the access control information from the content portion for use in the response message.

5. A method according to claim 2 wherein a hidden content is used in the response message to contain the access control information.

6. A method according to claim 1 further comprising presenting an option to the end user device to send the second message or not.

7. A method according to claim 2 wherein the response message's content portion is formatted as a custom content type.

8. A method according to claim 2 wherein at least part of the content portion of the response message is protected by cryptographic means.

9. A method according to claim 1 wherein the first message is an HTTP Request message, and the response message is an HTTP Response message.

10. A method according to claim 1 wherein the access control information is a cookie.

11. A method according to claim 1 further comprising:

containing user-specific information in the response message together with instructions to include at least part of the user-specific information in the second message.

12. A method according to claim 11 further comprising presenting an option to the end user device to change and/or delete any of the user-specific information before sending the message to the another network device.

13. A method according to claim 1 wherein the one network device is an initial network device accessed by the end user device, the method further comprising:

prior to sending the response message,

a) the initial network device receiving an initial access request from the end user device to access a protected resource on the initial network device;

b) the initial network device performing an authentication process to determine if access should be granted and if so, responding with an access response message specifying the access control information in association with the domain of the initial network device and causing the end user device to send the first message; and

on an ongoing basis after performing the authentication process allowing subsequent access to the protected resource to requests containing the access control information.

14. A method according to claim 13 further comprising:

containing user-specific information in the response message together with instructions to include at least part of the user-specific information in the second message.

15. A method according to claim 14 wherein the user-specific information comprises at least one of purchase enabling information and personal data.

16. A method according to claim 15 further comprising requiring user acceptance before including the at least part of the user-specific information in the second message.

17. A method according to claim 14 wherein at least part of the user-specific information is protected by cryptographic means.

18. A network device implemented method comprising:

a) a network device on a first network domain receiving an input message having a header portion and a content portion, with the input message containing an access control information embedded within the content portion;

b) the network device responding with a response message having a header portion and a content portion, with the response message containing the access control information in the header portion and having a content portion containing the access control information and also containing instructions to send a subsequent message to another network device on a different network domain, the subsequent message having a content portion containing at least part of the access control information.

19. A method according to claim 18 wherein the another network device is specified in the input message.

20. A method according to claim 18 wherein the another network device is specified by the network device.

21. A network device implemented method comprising:

the network device responding to an initial access request with a redirect message instructing a redirection to a MDSSO (multi-domain single sign-on) function on the network device, the redirect message also specifying an access control information in a header of the redirect message;

the MDSSO function receiving an input message having a header portion and a content portion, with the input message containing the access control information embedded within the header portion;

the MDSSO function responding with a response message having a header portion and a content portion, with the response message containing the access control information in the header portion and having the content portion containing the access control information and also containing instructions to send a subsequent message to another network device on a different network domain, the subsequent message having a content portion containing at least part of the access control information.

22. A method according to claim 21 further comprising performing an authentication process to determine if access should be granted, and if so responding to the initial access request message with the redirect message, and if not rejecting the initial access request.

23. A network device comprising an authentication front end and an MDSSO function, the network device being adapted to provide initial network device functionality upon receipt of a request message containing access control information only in a header portion, and adapted to provide non-initial network device functionality upon receipt of a request message

containing access control information in both a header portion and a content portion;

wherein in providing the initial network device functionality:

a) the authentication front end is adapted to process an initial access request message from an end user device to access a protected resource on the network device by performing an authentication process to determine if access should be granted and if so, responding with an access response message specifying an access control information in association with the domain of the network device and causing the end user device to send a first request message to an MDSSO (multiple domain single sign-on) function on the network device specifying the access control information in a header portion of the first request message;

b) the MDSSO function is adapted to process a request message directed to it containing access control information only in a header portion by extracting the access control information from the header portion and sending to the end-user device a response message containing the access control information in a header portion and having a content portion containing the access control information and also containing instructions to send a subsequent request message to another network device on a different network domain, the subsequent message having a content portion containing the at least part of access control information;

wherein in providing non-initial network device functionality:

c) the MDSSO function is adapted to process a request message directed to it containing access control information in a content portion by extracting the access control information from the content and sending to the end-user device a response message containing the access control information in a header

portion and having a content portion containing the access control information and also containing instructions to send a subsequent message to another network device on a different network domain, the subsequent message having a content portion containing at least part of the access control information.

24. A network device adapted to implement the method of claim 1.

25. A network device adapted to implement the method of claim 18.

26. An article of manufacture comprising:

a computer usable medium having computer readable program code means embodied therein for implementing the method of claim 1.

27. A multiple domain single sign-on system comprising a plurality of network devices according to claim 23.

28. The system of claim 27 wherein each of the plurality of network devices identifies a respective another network devices in the plurality of network devices.

29. The system of claim 27 wherein each response message identifies all remaining unvisited network devices in the plurality of network devices.

30. The system of claim 27 wherein each response message identifies all the network devices in the plurality of network devices.

31. An article of manufacture comprising:

a computer usable medium having computer readable program code means embodied therein for implementing a multiple domain single sign-on function, the computer readable code means in the article of manufacture comprising:

first computer readable code means adapted to receive in a first domain a first request message from a remote device and to generate a response message having a content portion, the content portion containing access control information and containing instructions causing the remote device to access a network address in a different domain specified in the content portion with a subsequent message containing at least part of the access control information.

32. An article of manufacture according to claim 31 further comprising:

second computer readable code means adapted to receive an access request message from the remote device, to perform authentication, and to send instructions to the remote device to send the first request message to the first computer readable code means.

33. An article of manufacture according to claim 32 wherein the access control information is generated by the second computer readable code means, sent to the remote device with the instructions, and then received by the first computer readable code means in the first request message.

34. A computer data signal embodied in a transmission medium comprising:

a first source code segment adapted to receive at a first domain a first request message from a remote device and to generate a response message having a content portion, the content portion containing access control information and

containing instructions to the remote device to access a network address at a different domain specified in the content portion with a subsequent message containing at least part of the access control information.

35. A method of conveying user-specific information from one network device to another network device on a different domain through an end user device comprising:

the one network device in response to a first message received from the end user device containing user-specific information, sending a response message to the end user device containing the user-specific information, the response message being adapted to cause the end user device to send a second message to the another network device containing at least part of the user-specific information after presenting an option to the end user device to change and/or delete any of the user-specific information;

wherein the response message has a header portion and a content portion and the response message contains the user-specific information and a network device identifier for the another network device embedded within its content portion;

the second message has a header portion and a content portion and the second message contains the at least part of the user-specific information embedded within its content portion.